

## **REMARKS**

Applicant respectfully traverses and requests reconsideration.

Claims 1, 15, 18, 20 and 24 are objected to due to an informality. However, it appears that the Examiner is referring to a previous amendment and not the past amendment. The past amendment included the words “at least one” and as such, the objection appears to be a mistake. However, if the objection is not a mistake, Applicant respectfully requests clarification as to why the current claims have informalities. In addition as to claim 15, lines 10-11, Applicant’s previous amendment already deleted “of the recipient”. Again, it appears that the objections are referring to a previous form of the claims and not the current form. As such, Applicant respectfully requests withdrawal of the objections.

Claims 1-8, 10, 12, 15-24 and 28 stand rejected under 35 U.S.C. §102(e) as being anticipated by Perlman et al. The independent claims have been amended to include inherent language since the claims refer to, inter alia, using a public key of the secure distribution server that is used to encrypt the secret key. In the original claim language, public key associated with the secure distribution server means the same thing. In any event, Perlman fails to teach all of the limitations of the claims. In the “Response to Amendment and Arguments” section, the section again fails to identify teachings in Perlman that teach the claimed subject matter. Instead, this section appears to admit that Perlman does not teach the claimed subject matter. For example, it is stated “It is not beyond the scope of his invention that a public key which corresponds to a specific intended recipient is used in place of a group secret key 314”. The reference itself must disclose the subject matter either expressly or inherently. The invention described in Perlman does not teach the claimed subject matter since the “scope” of this invention is set forth in the four corners of the Perlman reference. The office action admits that

Perlman does not teach what is alleged but apparently relies on the fact that somehow the teachings would not be “beyond the scope” of Perlman. However, the test is whether the Perlman reference teaches the claimed subject matter either expressly or inherently. It does neither. In addition, in the same section it is stated that “It should be appreciated that if a recipient’s public key was used to encrypt...”. Again, the allegation admits that Perlman does not teach it, but “if” Perlman did teach it, the claim would be anticipated. Such an argument should not be used to reject Applicant’s claims.

In any event, the office action also alleges that Perlman teaches, receiving an encrypted secret key encrypted using a public key, i.e. public key 107, associated with the secure distribution server, i.e. DLE 110 and group server 114 (column 5, lines 28-31 and column 7, lines 41-59). (Page 4 of office action). However, Perlman specifically states that public key 107 is “group public key 107”. “Group public key 107 is part of a public key – private key pair that is associated with a group of valid recipients from message 105.” (Column 5, lines 30-35). The group public key 107 is not associated or does not correspond to a secure distribution server as required in the claim. As such, Perlman does not teach the claimed subject matter. In fact, the cited group public key 107 that is alleged to correspond to the secure distribution server public key corresponds to a group of recipients and is always used to encrypt the group private key. There is no public key used by the DLE 110 or group server 114 in the cited portions that encrypt the secret key as alleged. The group public key 107 of Perlman is independent of the DLE and group server 114.

Applicant claims an encrypted secret key that is encrypted using a public key associated with a secure distribution server. For example, see Specification paragraph 22 and elsewhere noting that the public key associated with the secure distribution server (PKSDS) is used to

encrypt the secret key. No such DLE key or group server key is described or utilized to encrypt the secret key of Perlman as claimed. If the rejection is maintained, Applicant respectfully requests a showing by column and line number of where Perlman teaches the claimed subject matter. As such, Applicant respectfully submits that the independent claims are in condition for allowance.

Applicant also respectfully notes that the Response to Arguments section of the Final Action does not address Applicant's remarks with respect to claim 4 and other claims. As such, these claims are also in condition for allowance.

The dependent claims add additional novel and non-obvious subject matter. For example, claim 4 requires that the secret key is encrypted with the public key associated with the secure distribution server to produce the encrypted secret key and sending the encrypted information and the encrypted secret key to the secure distribution server. As such, the secure distribution server receives an encrypted secret key and encrypted information wherein the encrypted secret key that it receives is encrypted with a public key of the secure distribution server so that the secure distribution server can use its private key to decrypt the secret key. The secure distribution server is a trusted entity since the sender uses the public key of the secure distribution server to encrypt the secret key. Such operation as noted above is not taught in the cited portions of Perlman.

In addition, claim 5 requires that the secret key is encrypted using a public key for each of a plurality of secure distribution servers to produce a plurality of secure distribution server specific encrypted secret keys. The office action cites FIG. 4a-4c and column 4, lines 47-51 as allegedly teaching this subject matter. However, the cited portion merely states that a plurality of servers are involved in the process of encrypting and forwarding email messages. As set forth

throughout the specification of Perlman which actually describes the actual implementation of Perlman, and as noted above, there is no secure distribution server public key that is used to encrypt the secret key in the cited portions. In fact, as mentioned above with respect to FIG. 4a, it is only a group recipient key that is used in the initial encryption of the secret key process in Perlman. Such a key is independent of the DLE and group server 114 alleged to equate with the claimed secure distribution server. Accordingly, Applicant respectfully submits that there are no public keys for each of the secure distribution servers in Perlman and as such, this claim is also in condition for allowance.

The other dependent claims add additional novel and non-obvious subject matter.

Claims 9, 13 and 25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Perlman. Applicant respectfully submits that the mere forwarding and routing packets by nodes in the network is not equivalent to what is being claimed. Applicant respectfully notes that the claims cannot be parsed in such a manner as to ignore specific claim language. For example, in the context of claim 9 which depends on claim 1, not only is encrypted information received from a sender the encrypted key using a public key of the secure distribution server is also received. Also, the claim includes receiving the encrypted information and the encrypted secret key and forwarding the same to the secure distribution server without decrypting the encrypted secret key. Since the rejection of claim 1 attempts to equate the DLE and group server 114 of Perlman with the claimed secure distribution server, claim 9 requires that the encrypted information is also forwarded to the secure distribution server. However, the teachings of Perlman would not allow the forwarding and routing of packets in the nodes in a network to take effect as alleged in the office action since Perlman in fact teaches not to send the encrypted message to the group server. For example, as shown in FIG. 3, all that the group server receives

is the encrypted message key. The recipient performs the decryption and receives the encrypted message. As such, blindly including the forwarding and routing of packets as alleged in the office action to that of Perlman would materially change the operation of Perlman which as admitted in Perlman "can greatly compromise the system security" (see column 6, lines 1-8). Applicant respectfully submits that the combination as alleged is incompatible with the teachings of Perlman and as such, the claims are in condition for allowance.


Claims 11 and 27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Perlman in view of Chen. Applicant respectfully reasserts the relevant remarks made above with respect to Perlman and as such, these claims are also in condition for allowance.

Claim 14 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Perlman in view of Bouchard et al. Applicant respectfully reasserts the relevant remarks made above with respect to Perlman and as such, this claim is also in condition for allowance. The claim also adds additional novel and non-obvious subject matter.

Applicant respectfully requests that a timely Notice of Allowance be issued in this case. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

Date: 10-30-07

By:   
Christopher J. Rockamp  
Registration No. 34,414

Vedder, Price, Kaufman & Kamholz, P.C.  
222 N. LaSalle Street  
Chicago, Illinois 60601  
PHONE: (312) 609-7599  
FAX: (312) 609-5005